**system.sh**

#!/bin/bash

# INSTRUCTIONS: Edit the following placeholder command and output filepaths

# For example: cpu\_usage\_tool > ~/backups/cpuuse/cpu\_usage.txt

# The cpu\_usage\_tool is the command and ~/backups/cpuuse/cpu\_usage.txt is the filepath

# In the above example, the `cpu\_usage\_tool` command will output CPU usage information into a `cpu\_usage.txt` file.

# Do not forget to use the -h option for free memory, disk usage, and free disk space

# Free memory output to a free\_mem.txt

free -h > ~/backups/freemem/free\_mem.txt

# Disk usage output to a disk\_usage.txt file

du -h > ~/backups/diskuse/disk\_usage.txt

# List open files to a open\_list.txt file

lsof > ~/backups/openlist/open\_list.txt

# Free disk space to a free\_disk.txt file

df -h > ~/backups/freedisk/free\_disk.txt

**logrotate configuration file**

/var/log/auth.log {

weekly

rotate 7

notifempty

delaycompress

missingok

endscript

}

# see "man logrotate" for details

# rotate log files weekly

#weekly

# use the syslog group by default, since this is the owning group

# of /var/log/syslog.

#su root syslog

# keep 4 weeks worth of backlogs

#rotate 4

# create new (empty) log files after rotating old ones

#notifempty

# uncomment this if you want your log files compressed

#delaycompress

# packages drop log rotation information into this directory

#include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here

#/var/log/wtmp {

# missingok

# monthly

# create 0664 root utmp

# rotate 1

#}

#/var/log/btmp {

# missingok

# monthly

# create 0660 root utmp

# rotate 1

#}

# system-specific logs may be configured here

**Command to set number of retained logs and maximum log file size**

#

# This file controls the configuration of the audit daemon

#

local\_events = yes

write\_logs = yes

log\_file = /var/log/audit/audit.log

log\_group = adm

log\_format = RAW

flush = INCREMENTAL\_ASYNC

freq = 50

max\_log\_file = 35

num\_logs = 7

priority\_boost = 4

disp\_qos = lossy

dispatcher = /sbin/audispd

name\_format = NONE

##name = mydomain

max\_log\_file\_action = ROTATE

space\_left = 75

space\_left\_action = SYSLOG

verify\_email = yes

action\_mail\_acct = root

admin\_space\_left = 50

admin\_space\_left\_action = SUSPEND

disk\_full\_action = SUSPEND

disk\_error\_action = SUSPEND

use\_libwrap = yes

##tcp\_listen\_port = 60

tcp\_listen\_queue = 5

tcp\_max\_per\_addr = 1

##tcp\_client\_ports = 1024-65535

tcp\_client\_max\_idle = 0

enable\_krb5 = no

krb5\_principal = auditd

##krb5\_key\_file = /etc/audit/audit.key

distribute\_network = no

**Command using auditd to set rules for /etc/shadow, /etc/passwd and /var/log/auth.log**

**root@UbuntuDesktop:/etc# sudo cat /etc/audit/rules.d/audit.rules**

## First rule - delete all

-D

## Increase the buffers to survive stress events.

## Make this bigger for busy systems

-b 8192

## This determine how long to wait in burst of events

--backlog\_wait\_time 0

## Set failure mode to syslog

-f 1

## monitor shadow and passwd for any modifications or deletions

-w /etc/shadow -p wra -k hashpass\_audit

-w /etc/passwd -p wra -k userpass\_audit

-w /var/log/auth.log -p wra -k authlog\_audit

-w /var/log/cron -p wra

You have new mail in /var/mail/root